

The University of Chicago

REPRESENTATION OF BINARY FORMS
BY SETS OF TERNARY FORMS

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1936

By
DANIEL MACCABAEUS DRIBIN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
TRAVAUX DE L'INSTITUT MATHÉMATIQUE DE TBILISSI
Vol. 5, 1938

The University of Chicago

REPRESENTATION OF BINARY FORMS
BY SETS OF TERNARY FORMS

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1936

By

DANIEL MACCABAEUS DRIBIN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
TRAVAUX DE L'INSTITUT MATHÉMATIQUE DE TBILISSI
Vol. 5, 1938



REPRESENTATION OF BINARY FORMS BY SETS OF TERNARY FORMS

By D. M. DRIBIN (New Haven, Conn., U. S. A.)

1. *Introduction.* Let

$$(1) \quad f(x_1, x_2, x_3) = ax_1^2 + bx_2^2 + cx_3^2 + 2rx_2x_3 + 2sx_1x_3 + 2tx_1x_2$$

be a primitive integral classic ternary quadratic form with invariants¹⁾ Ω and Δ and determinant $d = \Omega^2 \Delta$.

Consider the replacements

$$(2) \quad x_i = a_i y_1 + b_i y_2 \quad (i = 1, 2, 3)$$

where the a_i and b_i are integers, and make these replacements in (1); then f becomes a classic binary form

$$\varphi = \alpha y_1^2 + 2\beta y_1 y_2 + \gamma y_2^2$$

where α, β, γ are certain quadratic functions of the a_i and b_i . The binary φ is said to be *represented* by f and the *representation* is said to be *proper* in case the two-rowed determinants of the matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

have greatest common divisor unity.

In case $f(x_1, x_2, 0) = \varphi(x_1, x_2)$ we shall say, as is customary, that φ is a section of f . Obviously, if φ is a section of f , it is represented properly by f .

We shall say that a binary form²⁾ φ is *represented* by (is a *section* of) the set $\Sigma(d)$ of all (classic) ternary forms²⁾ of determinant d in case there exists a ternary f of determinant d which represents φ (of which φ is a section). In the present paper we shall investigate the conditions for the repre-

¹⁾ The definitions of the invariants of a primitive classic ternary quadratic form are given in Chapter I of L. E. Dickson's *Studies in the theory of numbers* (Chicago, 1930).

²⁾ «Form» will henceforth mean «classic form».

sensation of a binary form $\varphi = (a, t, b)$, $t^2 - ab \neq 0$ by such a set $\Sigma(d)$ as has been described³⁾.

2. *Some known results. Reduction of the problem to proper representation.* For convenience we shall state at this point a few simple results concerning the representation of binary forms by ternaries⁴⁾.

LEMMA 1. *If φ is represented properly by f , then every binary equivalent to φ is also represented by f . Equivalent ternary forms represent properly the same binary forms.*

LEMMA 2. *If (2) is a proper representation of a binary form of determinant δ by a ternary f , having invariants Ω and Δ and reciprocal form F , then $\delta = -\Omega C$, where C is represented properly by F .*

LEMMA 3. *Let (2) be a proper representation of $\varphi = (a, t, b)$ of determinant $\delta \neq 0$ by a primitive ternary f whose invariants are Ω and Δ (whence, by Lemma 2, $\delta = -\Omega C$). Then f is equivalent to a form g of which φ is a section and such that the congruences*

$$R^2 + \Delta a \equiv 0, RS - \Delta t \equiv 0, S^2 + \Delta b \equiv 0 \pmod{C}$$

are simultaneously solvable.

Employing a result obtained by Gauss in his study of the representation of a binary form by a given ternary form, we can now reduce our problem effectively to the study of the proper representation of forms φ by sets $\Sigma(d)$.

Let φ be a binary form of determinant δ and let m^2 be a square divisor of δ . Let $\mathcal{A}_m$ connote the complex of all integral forms obtained from φ by a linear transformation of the form

$$\begin{pmatrix} \rho^{-1} & -\lambda m^{-1} \\ 0 & \sigma^{-1} \end{pmatrix}$$

where ρ and σ are positive integers, $\rho\sigma = m$, $\lambda = 0, 1, \dots, \sigma - 1$. Then the result⁵⁾ of Gauss to which we have already referred is equivalent to the

THEOREM 1. *A binary form φ of determinant δ is represented by a set $\Sigma(d)$ of classic ternaries if and only if there exists a square m^2 dividing δ such that $\mathcal{A}_m$ contains a form properly represented by $\Sigma(d)$.*

³⁾ A. A. Albert in *Amer. Journ. Math.*, LV (1933), 274 studied the representation of positive integers by a set $\Sigma(d)$ of positive classic ternaries. O. K. Sagen in his Chicago doctoral dissertation (1934), subsequently published in *Amer. Journ. Math.*, LIX (1937), 33 treated the same problem for non classic ternaries. These problems are, however, different, in several respects from the one treated in this paper; cf. § 4.

⁴⁾ The following three lemmas are proved in Dickson, op. cit., chap. 3.

⁵⁾ Gauss, *Disquisitiones Arithmeticae* (Maser's translation), 315—318.

3. *Proper representations of primitive binary forms.* Let $\varphi=(a, t, b)$ be represented properly by f , a ternary form of determinant d . If $f=ng$, where g is primitive, then n divides a, t, b . Hence $\Phi=\varphi/n$ is a classic binary form that is represented properly by the primitive ternary g .

By Lemma 3 Φ is a section of $\Sigma(d/n^3)$ so that $\varphi=n\Phi$ is a section of $\Sigma(d)$ and hence of some ternary h of determinant d . Then there exists integers r, s, c such that

$$(3) \quad d+ar^2+bs^2-2rst=(ab-t^2)c.$$

Conversely, if there exist integral solutions r, s, c of (3), then $\varphi=(a, t, b)$ is represented properly by $\Sigma(d)$. We have, then, the

THEOREM 2. *A binary form $\varphi=(a, t, b)$ is represented properly by a set $\Sigma(d)$ of classic ternaries if and only if φ is a section of $\Sigma(d)$. This condition will be satisfied if and only if there exist integral solutions r, s, c of the diophantine equation (3)⁶⁾.*

From (3) it follows immediately that if a, t, b have a common divisor $k>1$, then d is divisible by k so that we have

THEOREM 3. *If $\varphi=(a, t, b)$ is a section of $\Sigma(d)$ and if the greatest common divisor of a, t, b is k , then d is divisible by k and φ/k is a section of $\Sigma(d/k)$.*

In view of the foregoing theorem we shall restrict our attention at present to the representation of *primitive* binaries and shall later return to the consideration of the more general case.

LEMMA 4. *If $\varphi=(a, t, b)$ is a primitive binary of determinant $\delta \neq 0$, then φ is equivalent to a form $\Phi=(A, T, B)$ having T (and hence AB) relatively prime to δ .*

Since φ is primitive, it is equivalent to a form $\varphi'=(a', t', b')$ where a' is an integer relatively prime to δ . Furthermore, the transformation $x=x'+\alpha y'$, $y=y'$ carries φ' into the parallel form $\Phi=(A, T, B)$, where $T=a'\alpha+t'$ and if α is chosen so that $T=a'\alpha+t'$ is relatively prime to δ , we have the statement in the lemma.

By Lemma 1 φ is represented by a set $\Sigma(d)$ if and only if Φ is, so that we need consider only those primitive forms $\varphi=(a, t, b)$ of determinant $\delta \neq 0$ with $(t, \delta)=1$.

Let φ be represented properly by a set $\Sigma(d)$ so that there exists a primitive ternary $f(x, y, z)$ of determinant d of which φ is a section. Write $f=ax^2+by^2+cz^2+2ryz+2sxz+2txy$ and let Ω and Δ be the invariants of f . Then by Lemmas 2 and 3, $\delta=-\Omega C$, with C an integer, and the congruences

⁶⁾ In view of this theorem we shall, for the most part, employ the shorter phrase «is a section of» rather than «is represented properly by».

$$(4) \quad R^2 + \Delta a \equiv 0, \quad RS - \Delta t \equiv 0, \quad S^2 + \Delta b \equiv 0 \pmod{C}$$

are solvable for R and S .

By the definition of Ω , it follows at once⁷⁾ that

$$(5) \quad ar - ts = -\Omega R, \quad tr - bs = \Omega S,$$

or, what is the same thing, by solving (5) for r, s , and imposing the condition that r and s be integers, we obtain

$$(6) \quad bR + tS \equiv 0, \quad tR + aS \equiv 0 \pmod{C}.$$

Since by (3) and (5)

$$\begin{aligned} c &= \frac{d + ar^2 + bs^2 - 2rst}{ab - t^2} = \frac{\Omega^2 \Delta + r(ar - ts) + s(bs - tr)}{\Omega C} \\ &= \frac{\Omega \Delta - rR - sS}{C} \end{aligned}$$

we have, furthermore, that

$$(7) \quad \Omega \Delta - rR - sS \equiv 0 \pmod{C}.$$

Conversely, let $\varphi = (a, t, b)$ be primitive and of determinant δ and let d be an integer. If there exist divisors of d and δ defined by $d = \Omega^2 \Delta$, $\delta = -\Omega C$, such that the congruences (4) and (6) (and hence (5)) have solutions, then φ is a section of $\Sigma(d)$.

For, (4), (5), (6) imply (7) since

$$\begin{aligned} a(\Omega \Delta - rR - sS) &\equiv \Omega \Delta a - arR - asS \\ &\equiv -\Omega R^2 - R(-\Omega R + st) - asS \\ &\equiv -s(tR + aS) \equiv 0 \pmod{C} \end{aligned}$$

and a is prime to $\delta = -\Omega C$.

Hence a form f representing φ properly is furnished by (1), where c is defined as the quotient of the left member of (7) by C .

THEOREM 4. *A primitive binary $\varphi = (a, t, b)$ of determinant $\delta \neq 0$ is a section of $\Sigma(d)$ if and only if there exist divisors Δ and C of d and δ respectively, defined by $d = \Omega^2 \Delta$, $\delta = -\Omega C$, such that (4) and (6) have integral solutions R, S .*

⁷⁾ The coefficients R, S and C in the reciprocal F to f satisfy (4) and (5).

As an immediate consequence from the proof of Theorem 4 we have the

THEOREM 5. *A primitive binary $\varphi=(a, t, b)$ of determinant $\delta \neq 0$ is a section of $\Sigma(d)$ if and only if the congruences*

$$(8) \quad R^2 + da \equiv 0, \quad RS - dt \equiv 0, \quad S^2 + db \equiv 0 \pmod{\delta}$$

$$(9) \quad bR + tS \equiv 0, \quad tR + aS \equiv 0 \pmod{\delta}$$

have integral solutions R, S .

We shall now show that of the five congruences (8), (9), we need retain only (8₁) so that we shall have the

THEOREM 6. *Let $\varphi=(a, t, b)$ be a primitive binary form of determinant $\delta \neq 0$, having t and δ relatively prime. Then φ is a section of the set $\Sigma(d)$ of all classic ternaries of determinant d if and only if the congruence $R^2 + da \equiv 0 \pmod{\delta}$ is solvable.*

To prove this assertion we need only note that if R_0 is a solution of (8₁) and S_0 a solution of $aS \equiv -tR_0 \pmod{\delta}$, then these solutions R_0, S_0 will satisfy the remaining congruences (8) and (9).

In the following, p is a prime divisor of δ and $\alpha = \alpha(p)$, $\beta = \beta(p)$ are the multiplicities of p in δ and $d = p^\beta d'$, respectively; as before, we may assume that the binary form $\varphi = (a, t, b)$, $t^2 - ab = \delta$, is subject to the restriction $(t, \delta) = 1$.

We may now state as a final proposition on the proper representation of primitive binaries the following theorem, which follows immediately from the preceding Theorem 6.

THEOREM 7. *Let $\varphi=(a, t, b)$ be a primitive binary of determinant $\delta \neq 0$, subject to the restrictions above. Then φ is a section of the set $\Sigma(d)$ of all classic ternaries of determinant d if and only if*

(1) $\beta < \alpha$ for any prime p dividing δ implies β is even,

(2) $(-d'a|p) = 1$ for every odd prime p dividing δ for which $\beta < \alpha$,

(3) if $\beta(2) < \alpha(2)$, $-d'a \equiv 1 \pmod{2^k}$, where $k=2$ or 3 according as $\alpha - \beta = 2$ or $\alpha - \beta \equiv 3$, respectively.

It may be remarked, in passing, that in consequence of Theorem 7 the genus of φ is represented properly by $\Sigma(d)$ whenever φ is. In general, of course, all the genera of a given determinant are not simultaneously represented properly by a set $\Sigma(d)$.

4. *Representation of primitive binary forms.* As in the preceding section we shall assume that φ is primitive so that we may take its first coefficient a prime to δ .

By Theorem 1 and the discussion immediately preceding it, the form $\varphi=(a, t, b)$ is represented by $\Sigma(d)$ if and only if there exists a square m^2 dividing δ such that the binary

$$(10) \quad a\rho^{-2}x^2 - 2(a\rho^{-1}m^{-1}\lambda - t\sigma^{-1}\rho^{-1})xy + (a\lambda^2m^{-2} - 2t\sigma^{-1}m^{-1}\lambda + b\sigma^{-2})y^2$$

is an integral form that is a section of $\Sigma(d)$, where ρ and σ are positive integers, $\rho\sigma = m$, $\lambda = 0, 1, \dots, \sigma - 1$.

Since a is prime to δ , $a\rho^{-2} = a$, so that (10) becomes

$$(11) \quad ax^2 - 2(a\lambda - t)m^{-1}xy + (a\lambda^2 - 2t\lambda + b)m^{-2}y^2.$$

The coefficients of xy and y^2 in (11) are, however, uniquely determined, for the congruence $a\lambda - t \equiv 0 \pmod{m}$ determines λ , and

$$(a\lambda - t)^2 = a^2\lambda^2 - 2at\lambda + t^2 \equiv a(a\lambda^2 - 2t\lambda + b) \equiv 0 \pmod{m^2}.$$

But $(a\lambda^2 - 2t\lambda + b)m^{-2}$ is the third coefficient of (11).

By the kernel of δ shall be understood the greatest quadratfrei divisor δ_0 of δ . It should then be obvious that if Theorem 7 holds for the form (11) of determinant δ/m^2 it will also hold if δ/m^2 be replaced by δ_0 , by choosing

m^2 to be the greatest square $\frac{\delta}{\delta_0} = \bar{\delta}^2$ dividing δ . For, the only odd primes p

affected in Theorem 7 are those for which $\beta(p) < \alpha(p)$, and the prime 2 is affected only if $\alpha(2) - \beta(2) \equiv 2$. Consequently, in the process of removing square factors from δ/m^2 to form δ_0 , an odd prime p either retains the property $\beta(p) < \alpha(p)$ (where α refers to δ_0) or $\beta(p) \equiv \alpha(p)$, which is no longer a condition by Theorem 7. A similar statement applies to factors of 4 in δ/m^2 .

Conversely, if (11) of determinant δ_0 is a section of $\Sigma(d)$, φ is represented by $\Sigma(d)$. For, then $\delta = \delta_0 \bar{\delta}^2$ and by hypothesis there exists a square $\bar{\delta}^2$ dividing δ such that the form (11) of determinant $\delta/\bar{\delta}^2 = \delta_0$ is represented properly by $\Sigma(d)$. But by the criterion of Gauss, φ is then represented by $\Sigma(d)$.

Hence we have the

THEOREM 8. Let $\varphi = (a, t, b)$ be a primitive binary of determinant $\delta \neq 0$ and with $(t, \delta) = 1$. Then φ is represented by a set $\Sigma(d)$ if and only if $(-da|p) = 1$ for every odd prime p dividing the kernel of δ that is prime to d .

5. Proper representation of imprimitive binary forms. By Theorem 3 a necessary condition that a binary $\psi = k\varphi$ be a section of a set $\Sigma(kd)$ of classic ternaries is that φ itself be a section of $\Sigma(d)$. Since φ may be taken to be primitive and since in § 3 we had determined the criteria for the proper representation of such a form by $\Sigma(d)$, the question to which we now seek an answer is: If $\varphi = (a, t, b)$, a primitive binary form of determinant $\delta \neq 0$, is a section of $\Sigma(d)$, what are necessary and sufficient conditions that $\psi = k\varphi$ be a section of $\Sigma(kd)$?

We have the

LEMMA 5. If $\varphi = (a, t, b)$ is a section of $\Sigma(d)$, then a necessary and sufficient condition that $k\varphi$ be a section of $\Sigma(kd)$ is that there exist solutions r, s and c of (3) with c divisible by k .

That the condition is necessary is immediate from (3). Conversely, if $c=kc_0$, r, s are solutions of (3) with c_0 an integer, then

$$kd + (ka)r^2 + (kb)s^2 - 2rs(kt) = [(ka)(kb) - (kt)^2]c_0$$

and by Theorem 2 $k\varphi$ is a section of $\Sigma(kd)$.

It might be wise, perhaps, to digress at this point and enlarge somewhat on the differences between our problem and that of A. A. Albert in his paper entitled «*The integers represented by sets of ternary quadratic forms*» which appeared in the *American Journal of Mathematics* for 1933. In that paper, as in ours, the diophantine equation (3) appears, the solution of which is the *Leitfaden* of the investigation, but important differences occur. Whereas the integers d, a, t, b in our problem are, in a sense, fixed, such was not the case in the problem Albert treated, for there a and d are alone fixed. It is true that Albert, since he was concerned with sets $\Sigma(d)$ of *positive* ternary forms, imposed the restrictions $d > 0$, $ab - t^2 > 0$, but these restrictions were not of such a nature as to prevent the simplification of many features of his work. It cannot be too strongly emphasized that $ab - t^2$ in Albert's paper *was not a fixed quantity* and so left open much room for simplification of the problem. For example, in the paper of Sagen, to which we have already referred, the coefficient t could be taken to be zero with no resulting loss of generality.

It is almost superfluous to add, then, that due to the tightening of the conditions in our problem and hence the reduction of the freedom permitted us, many such simplifications could not be effected. It need not be surprising, therefore, that the following treatment of the proper representation of the imprimitive binaries results in much more detail and complication than the simple theory of the primitive binary as contained in Theorem 7.

We shall first let $k=p^e$, p an odd prime, and shall divide the following discussion into several cases and as many sections.

6. *Primes p not dividing $d\delta$.* We shall prove the

THEOREM 9. *If a primitive binary φ of determinant $\delta \neq 0$ is a section of a set $\Sigma(d)$ and if p is an odd prime not dividing $d\delta$, then $p^e\varphi$ is a section of $\Sigma(p^e d)$ for every $e > 0$.*

Since φ is primitive, it is easily seen that we may take $t \equiv 0 \pmod{p^e}$, whence, since $(\delta, p) = 1$, $ab \not\equiv 0 \pmod{p}$.

In order that $p^e\varphi$ be represented properly by $\Sigma(p^e d)$ it is sufficient, by Lemma 5, to show the existence of solutions r and s of the congruence

$$(12) \quad d + ar^2 + bs^2 - 2rst \equiv d + ar^2 + bs^2 \equiv 0 \pmod{p^e}.$$

To do this we employ the

LEMMA 6. *If $\Phi(x, y) \equiv 0 \pmod{p}$ is solvable modulo the prime p , then $\Phi(x, y) \equiv 0 \pmod{p^e}$ is solvable for every $e > 0$ if the congruences*

$$(13) \quad \Phi(x, y) \equiv 0, \quad \frac{\partial \Phi}{\partial x} \equiv 0, \quad \frac{\partial \Phi}{\partial y} \equiv 0 \pmod{p}$$

have no common sets of solutions (x, y) ⁸⁾.

The congruences (13) with $\Phi(x, y) = ax^2 + by^2 + d$ become

$$(14) \quad ax^2 + by^2 + d \equiv 0, \quad 2x \equiv 2y \equiv 0 \pmod{p},$$

which cannot be simultaneously satisfied, since p is odd and prime to d . But the congruence (13₁) is solvable, by virtue of the following theorem of Lagrange⁹⁾ and the fact $ab \not\equiv 0 \pmod{p}$.

LEMMA 7. *If $ab \not\equiv 0 \pmod{p}$, p an odd prime, the congruence $ax^2 + by^2 + d \equiv 0 \pmod{p}$ is solvable for every integer d .*

Combining Lemmas 6 and 7, we see that (12) is solvable. Since δ and p are relatively prime and since the congruence $d + ar^2 + by^2 - 2rst \equiv 0 \pmod{\delta}$ is solvable, by hypothesis, it follows that the congruence $d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{p^e \delta}$ is solvable, so that $p^e \varphi$ is a section of $\Sigma(p^e d)$.

7. *Primes p dividing δ but not d .* We shall prove the

THEOREM 10. *If a primitive binary φ of determinant $\delta \neq 0$ is a section of a set $\Sigma(d)$ and if p is an odd prime dividing δ but not d , then $p^e \varphi$ is a section of $\Sigma(p^e d)$ for every integer $e > 0$.*

We shall assume during this section that $abt \not\equiv 0 \pmod{p}$, as we have already done before.

By Theorem 6, $(-da|p) = 1$ so that the congruence $d + ar^2 \equiv 0 \pmod{p^{\alpha+e}}$ is solvable, where p^α is the highest power of p dividing δ . We choose $s \equiv 0 \pmod{p^{\alpha+e}}$. Then, since the congruence $d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{\delta/p^\alpha}$ is solvable by hypothesis, there exist integers r and s satisfying

$$(15) \quad d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{p^{\alpha+e}}, \quad \delta/p^\alpha = p^e \delta$$

and, by Lemma 5, $p^e \varphi$ is represented properly by $\Sigma(p^e d)$.

8. *Primes p dividing d but not δ .* Let β be the multiplicity of p in d and write $d = p^\beta d'$; we may assume that a is prime to p . The theorem we shall prove in this section is

THEOREM 11. *Let φ , a primitive binary form of determinant $\delta \neq 0$ be represented properly by a set $\Sigma(d)$ and let p be an odd prime dividing d but not δ . If β is even or if β is odd and $e = 1$, then $p^e \varphi$ is a section of $\Sigma(p^e d)$; but if β is odd and $e > 1$, then $p^e \varphi$ is a section of $\Sigma(p^e d)$ if and only if $(\delta|p) = 1$.*

⁸⁾ Hermite, *Journ. für Math.* 47 (1854), 353; Oeuvres 1, 245. For an application to a later section, it must be noted here that the conclusion of Lemma 6 will remain valid if only there exist one solution (x, y) of $\Phi(x, y) \equiv 0 \pmod{p}$ that does not satisfy (13) simultaneously.

⁹⁾ Cf. Dickson, *Annals of Math.*, (2), 28 (1927), 333.

We shall need the

LEMMA 8. *If a binary φ is represented properly by a set $\Sigma(d)$, then it is so represented by $\Sigma(m^2d)$ for every integer m .*

For, by Theorem 2, there exist integral solutions r, s, c of

$$(16) \quad d + ar^2 + bs^2 - 2rst = (ab - t^2)c$$

whence, by multiplying (16) by m^2 , we obtain

$$m^2d + a(mr)^2 + b(ms)^2 - 2(mr)(ms)t = (ab - t^2)(m^2c)$$

so that by the same theorem $\varphi = (a, t, b)$ is properly represented by $\Sigma(m^2d)$.

Let now $d \equiv 0 \pmod{b^2}$. There exists a solution η of the congruence $p\eta \equiv 1 \pmod{\delta}$ so that, since the congruence

$$d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{\delta}$$

is solvable for r and s by hypothesis, we get

$$d/p^2 + a(\eta r)^2 + b(\eta s)^2 - 2(\eta r)(\eta s)t \equiv 0 \pmod{\delta}$$

and φ is a section of $\Sigma(d/p^2)$. Continuing in this manner, we find that φ is represented properly by $\Sigma(d')$ or $\Sigma(pd')$ according as β is even or odd.

In the former case we note that since $(d', p) = 1$, we have reverted to the case of § 6, so that $p^e\varphi$ is a section of $\Sigma(p^e d')$ for every $e > 0$. But then by Lemma 8, $p^e\varphi$ is a section of $\Sigma(p^\beta \cdot p^e d') = \Sigma(p^e d)$.

Let, then, β be odd. In this case the binary $p^e\varphi$ is represented properly by $\Sigma(p^e pd')$ (and hence by $\Sigma(p^{\beta-1} p^e pd') = \Sigma(p^e d)$) if and only if there exist solutions r and s of the congruence

$$pad' + (ar - st)^2 - \delta s^2 \equiv 0 \pmod{p^e},$$

a condition which is equivalent, since a is prime to p , to the solvability of

$$(17) \quad pad' + x^2 - \delta y^2 \equiv 0 \pmod{p^e}.$$

But (17) is obviously solvable for $e = 1$. When $e > 1$ we utilize the remark to Lemma 6 and realize that (17) is solvable if and only if $(\delta|p) = 1$.

9. *Primes p dividing d and δ .* Let α and β be the respective multiplicities of p in δ and d and write $\delta = p^\alpha \delta'$, $d = p^\beta d'$. As in § 8, we may take a prime to p .

We shall first prove

THEOREM 12. *Let φ be primitive binary of determinant $\delta \neq 0$ properly represented by $\Sigma(d)$ and let p be an odd prime dividing d and δ . Then if $\beta < \alpha$ or if $e \equiv \beta - \alpha$, $p^e\varphi$ is represented properly by $\Sigma(p^e d)$.*

Let $\beta < \alpha$. Then, by Theorem 7, β is even and $(-d'a|p) = 1$ so that the congruence $d' + ar^2 \equiv 0 \pmod{p^{\alpha+e}}$ is solvable. If we choose $s \equiv 0$

(mod $p^{\alpha+e}$) as in § 7 and proceed as in that case, we obtain the conclusion of the theorem.

Let, then, $\beta \equiv \alpha$. By Theorem 5, the congruences (8), (9) are solvable. Since $\beta \equiv \alpha$, there exist solutions R and S with $R \equiv S \equiv 0 \pmod{p^{\beta+\alpha}}$. Hence

$$r = \frac{1}{\delta} (bR + tS), \quad s = \frac{1}{\delta} (tR + aS)$$

are integers and $r \equiv s \equiv 0 \pmod{p^\beta}$,

$$ar - ts = -R, \quad tr - bs = S.$$

Proceeding as in the proof of Theorem 4, we find

$$d - rR - sS \equiv 0 \pmod{\delta},$$

i. e. (3) is satisfied with

$$c = \frac{1}{\delta} (d - rR - sS),$$

where $c \equiv 0 \pmod{p^{\beta-\alpha}}$. Since $\beta - \alpha \equiv e$, $p^e \varphi$ is a section of $\Sigma(p^e d)$ by Lemma 5.

If $0 \equiv \beta - \alpha < e$, we write $d = p^{2\gamma} d''$, $r = p^\gamma r'$, $s = p^\gamma s'$, $c = p^{2\gamma} c'$, where $2\gamma = \beta - \alpha$ or $\beta - \alpha - 1$ according as $\beta - \alpha$ is even or odd. Then (3) becomes

$$d'' + ar'^2 + bs'^2 - 2r's't = (ab - t^2)c'$$

and φ is a section of $\Sigma(d'')$. As in § 8, $p^e \varphi$ is a section of $\Sigma(p^e d'')$ and hence of $\Sigma(p^e d)$ if and only if there exist solutions x, y of the congruence

$$(18) \quad ad'' + x^2 - \delta y^2 \equiv 0 \pmod{p^{\alpha+e}}.$$

We note, in passing, that according as $\beta - \alpha$ is even or odd, the highest power of p dividing d'' is $\beta - 2\gamma = \alpha$ or $\alpha + 1$ in the respective cases.

i. $\beta - 2\gamma = \alpha$, α even. Then $x = p^{\frac{\alpha}{2}} x'$ and we have $ad' + x'^2 - \delta' y^2 \equiv 0 \pmod{p^e}$. But this congruence is solvable for all e by § 6.

ii. $\beta - 2\gamma = \alpha + 1$, α even. As in i, we have that $apd' + x'^2 - \delta' y^2 \equiv 0 \pmod{p^e}$. When $e = 1$, this congruence is obviously solvable, but when $e > 1$ if and only if $(\delta' | p) = 1$.

iii. $\beta - 2\gamma = \alpha$, α odd. By (18), $x = p^{\frac{\alpha+1}{2}} x'$ and we get $ad' + px'^2 - \delta' y^2 \equiv 0 \pmod{p^e}$; this congruence is solvable if and only if $(ad' | p) = (\delta' | p)$.

iv. $\beta - 2\gamma = \alpha + 1$, α odd. As in iii, $x = p^{\frac{e+1}{2}} x'$ and we get $apd' + px'^2 - \delta'y'^2 \equiv 0 \pmod{p^e}$. When $e=1$, this congruence is solvable. If $e>1$, then $y=py'$ and $ad' + x'^2 - p\delta'y'^2 \equiv 0 \pmod{p^{e-1}}$; this congruence is solvable if and only if $(-ad'|p) = 1$.

We have, then, the

THEOREM 13. Let φ be a primitive binary of determinant $\delta \neq 0$ and a section of $\Sigma(d)$; let p be an odd prime dividing d and δ and let $\delta = p^\alpha \delta'$, $d = p^\beta d'$, where $(\delta'd', p) = 1$. We assume that $0 \leq \beta - \alpha < e$. Then if α and β are both even, the binary $p^e \varphi$ is a section of $\Sigma(p^e d)$ for every $e > 0$. If α is even and β odd, $p^e \varphi$ is a section of $\Sigma(p^e d)$ for $e=1$, but when $e>1$ if and only if $(\delta'|p) = 1$. If α is odd and β even, $p^e \varphi$ is a section of $\Sigma(p^e d)$ for $e=1$, but when $e>1$ if and only if $(-ad'|p) = 1$. Finally, if $\alpha\beta$ is odd, then $p^e \varphi$ is a section of $\Sigma(p^e d)$ if and only if $(ad'|p) = (\delta'|p)$.

10. Proper representation of $2^e \varphi$ by $\Sigma(2^e d)$. We shall now investigate the proper representation of $2^e \varphi$ by $\Sigma(2^e d)$ when φ is primitive and properly represented by $\Sigma(d)$. As before, if α is the multiplicity of 2 in δ and ε that in a (we may always take $\varepsilon=0$ if φ is properly primitive), $2^e \varphi$ will be a section of $\Sigma(2^e d)$ only if there exist solutions r, s of the congruence $ad + (ar-st)^2 - \delta s^2 \equiv 0 \pmod{2^{\alpha+\varepsilon+e}}$. Hence a necessary condition that $2^e \varphi$ be represented properly by $\Sigma(2^e d)$ is that there exist solutions x, y of

$$(19) \quad ad^2 + x^2 - \delta y^2 \equiv 0 \pmod{2^{\alpha+\varepsilon+e}}.$$

If φ is properly primitive, this necessary condition is obviously sufficient, for we may then take $\varepsilon=0$. But if φ is improperly primitive, an additional argument is necessary. Then $\delta \equiv t^2 - ab \equiv 1 \pmod{4}$ and with no loss of generality we may take $a \equiv 2 \pmod{4}$. For if $a \equiv b \equiv 0 \pmod{4}$ the form φ may be subjected to the linear transformation

$$x = X, \quad y = X + Y,$$

which transforms it into the parallel form $\Phi = (A, T, B)$ with $A = a + 2t + b \equiv 2 \pmod{4}$. Hence we may assume $\varepsilon=1$ in the case that φ is improperly primitive so that $\alpha + e + \varepsilon \geq e + 1 \geq 2$.

Hence, if (19) is solvable with φ improperly primitive, x and y must be both even or both odd. We choose $s \equiv y \pmod{2^{e+1}}$ and determine the solution r of $ar - st \equiv x \pmod{2^{e+1}}$. (Such a solution exists since $x + st$ is divisible by 2, the g. c. d. of a and 2^{e+1}). Then we have $d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{2^e}$ and $2^e \varphi$ is properly represented by $\Sigma(2^e d)$.

We conclude, therefore, that if φ is primitive and a section of $\Sigma(d)$ and if a is taken odd or $\equiv 2 \pmod{4}$ according as φ is properly or improperly primitive, the binary $2^e \varphi$ is a section of $\Sigma(2^e d)$ if and only if (19) is solvable.

THEOREM 14. Let $\varphi = (a, t, b)$ be a primitive binary of determinant $\delta \neq 0$ and a section of $\Sigma(d)$. Assume that $\beta(2) < \alpha(2)$. Then if $\alpha - \beta \equiv 2$ or if $\alpha - \beta = e = 1$, $2^e \varphi$ is a section of $\Sigma(2^e d)$. But if $\alpha - \beta = 1 < e$, $2^e \varphi$ is a section of $\Sigma(2^e d)$ if and only if one of the following sets of conditions is satisfied: $\delta' \equiv 1 \pmod{4}$, $ad' \equiv \pm 1 \pmod{8}$; $\delta' \equiv 3 \pmod{4}$, $ad' \equiv 5, 7 \pmod{8}$.

Since $\beta < \alpha$, β is even by Theorem 7. Also $\alpha > 0$, whence φ is properly primitive, and $\varepsilon = 0$ in (19) $\underline{\beta}$

i. $\alpha - \beta = 1$. By (19), $x = 2^2 x'$ and (19) becomes $ad' + x'^2 - 2\delta'y^2 \equiv 0 \pmod{2^{e+1}}$, which is solvable for $e = 1$. When $e > 1$ this congruence is solvable if and only if the conditions of the theorem hold.

ii. $\alpha - \beta = 2$. By Theorem 7, $-d'a \equiv 1 \pmod{4}$. If $-d'a \equiv 1 \pmod{8}$, $(ad' + x^2 \equiv 0 \pmod{2^{e+\alpha}})$ is solvable, so that (19) is also, with $y \equiv 0 \pmod{2^{e+\alpha}}$. If $-d'a \equiv 5 \pmod{8}$, then (19) implies $3 + x'^2 - 4\delta'y^2 \equiv 0 \pmod{8}$ and this congruence is always solvable, since δ' is odd.

iii. $\alpha - \beta \equiv 3$. By theorem 7, $-d'a \equiv 1 \pmod{8}$ and the congruence $ad' + x^2 - \delta'y^2 \equiv ad' + x^2 \equiv 0 \pmod{8}$ is solvable.

If $\beta \equiv \alpha$, we may again employ the notations $d = p^2 \gamma d''$, $\delta = p^\alpha \delta'$, where $2\gamma = \beta - \alpha$ or $\beta - \alpha - 1$ according as $\beta - \alpha$ is even or odd. Again, as in § 9, $2^e \varphi$ will be represented properly by $\Sigma(2^e d)$ if and only if there exist solutions x, y of

$$(20) \quad ad'' + x^2 - \delta'y^2 \equiv 0 \pmod{2^{\alpha+e+\varepsilon}}$$

where the conventions as to ε are retained.¹⁰⁾

THEOREM 15.*. Let $\varphi = (a, t, b)$ be a primitive binary of determinant $\delta \neq 0$ properly represented by $\Sigma(d)$ and let $\beta(2) \equiv \alpha(2)$. Necessary and sufficient conditions for the proper representation of $2^e \varphi$ by $\Sigma(2^e d)$ are

(1) when $0 \equiv \beta - \alpha < e$, α and β both even, $e + \varepsilon = 2$, that either $\delta' \equiv 1$, $ad' \not\equiv 2$ or $\delta' \equiv 3$, $ad' \not\equiv 1 \pmod{4}$,

(2) when α and β are both even, $e + \varepsilon > 2$, and either (i) $\alpha = \beta$ or (ii) $0 < \beta - \alpha < e + \varepsilon - 2$ when $\delta' \not\equiv 1 \pmod{8}$ that one of the following conditions obtain: $\delta' \equiv 1$, $ad' \not\equiv 2 \pmod{4}$; $\delta' \equiv 3$, $ad' \not\equiv 1, 5, 6 \pmod{8}$; $\delta' \equiv 7$, $ad' \not\equiv 1, 2, 5 \pmod{8}$,

(3) when α and β are both even, $e + \varepsilon > 2$, $0 < \beta - \alpha = e - 1$, $\delta' \equiv 5 \pmod{8}$, that $\varepsilon = 0$,

(4) when α and β are both even, $e + \varepsilon > 2$, $0 < \beta - \alpha = e + \varepsilon - 2$, $\delta' \not\equiv 1 \pmod{8}$, that one of the following hold: $\delta' \equiv 1$, $ad' \not\equiv 2$; $\delta' \equiv 3$, $ad' \not\equiv 1 \pmod{4}$,

¹⁰⁾ Hence $ad' \not\equiv 0 \pmod{4}$.

* The author wishes to express his appreciation for the critical and constructive suggestions made by Professor A. Walfisz relative to Theorem 15.

(5) when α is even, β odd, $\varepsilon=0$, and either $\beta-\alpha=1$, $e=2$, or $\beta-\alpha=e-1$, $e>2$, that $\delta'\equiv 3 \pmod{4}$,

(6) when α is even, β odd, $\beta-\alpha=1$, $e>2$, $\varepsilon=0$, that $\delta'\equiv 3 \pmod{4}$, and that $ad'\equiv 1 \pmod{4}$ when $\delta'\equiv 3 \pmod{8}$ and $ad'\equiv 3 \pmod{4}$ when $\delta'\equiv 7 \pmod{8}$,

(7) when α is even, β odd, $\delta'\not\equiv 1 \pmod{8}$, $\beta-\alpha\equiv e+\varepsilon-2$ that one of the following obtain: $\delta'\equiv 3 \pmod{8}$, $ad'\equiv 1 \pmod{4}$; $\delta'\equiv 5 \pmod{8}$, $\varepsilon=1$; $\delta'\equiv 7 \pmod{8}$, $ad'\equiv 3 \pmod{4}$,

(8) when $\alpha\beta$ is odd, $\varepsilon=0$, and either (i) $\alpha-\beta$, $e>2$ or (ii) $0<\beta-\alpha\equiv e-3$; that one of the following conditions obtain: $\delta'\equiv 1$, $ad'\equiv \pm 1$; $\delta'\equiv 3$, $ad'\equiv 1$, 3 , $\delta'\equiv 5$, $ad'\equiv 3, 5$; $\delta'\equiv 7$, $ad'\equiv 5, 7 \pmod{8}$,

(9) when $\alpha\beta$ is odd, $\varepsilon=1$ and either (i) $\alpha=\beta$, $e>2$, or (ii) $0<\beta-\alpha\equiv e-3$ that $ad'\equiv \pm 2 \pmod{16}$,

(10) when α is odd, β even, $\beta-\alpha=1$, $e>3$, $\varepsilon=0$ that either $ad'\equiv 7$ or that $ad'\equiv 1$ when $\delta'\equiv 1$ or 5 or that $ad'\equiv 5$ when $\delta'\equiv 3$ or $7 \pmod{8}$,

(11) when α is odd, β even, $\varepsilon=1$, and either $\beta-\alpha=1$, $e>3$ or $1<\beta-\alpha\equiv e-3$ that $ad'\equiv \pm 2 \pmod{16}$ when $\delta'\equiv 1 \pmod{8}$, and $ad'\equiv \pm 6 \pmod{16}$ when $\delta'\equiv 5 \pmod{8}$,

(12) when α is odd, β even, $\varepsilon=0$, $1<\beta-\alpha\equiv e-3$ that $ad'\equiv \pm 1 \pmod{8}$ for $\delta'\equiv 1 \pmod{4}$ and $ad'\equiv 5, 7 \pmod{8}$ for $\delta'\equiv 3 \pmod{4}$.

In all cases not included among (1)–(12) above (in particular, if $\beta-\alpha\equiv e$) $2^e\varphi$ is represented properly by $\Sigma(2^e d)$.

We shall first show that when $\beta-\alpha\equiv e$, (19) is always solvable.

i. α even. From (19) $x=2^{\frac{\alpha}{2}}x'$ and $2^{\beta-\alpha}ad'+x'^2-\delta'y^2\equiv 0 \pmod{2^{e+\varepsilon}}$. When $\varepsilon=0$, this congruence becomes $x'^2-\delta'y^2\equiv 0 \pmod{2^e}$ which is always solvable. When $\varepsilon=1$, α is even and we get $x'^2-\delta'y^2\equiv 0 \pmod{2^{e+1}}$, which is solvable.

ii. α odd. From (19) $x=2^{\frac{\alpha+1}{2}}x'$ and we get $2^{\beta-\alpha}ad'+2x'^2-\delta'y^2\equiv 0 \pmod{2^{e+\varepsilon}}$. When $\varepsilon=0$ we get $2x'^2-\delta'y^2\equiv 0 \pmod{2^e}$, which is solvable. When $\varepsilon=1$, we get $2x'^2-\delta'y^2\equiv 0 \pmod{2^{e+1}}$, which is also solvable.

Hence in the remainder of this proof we shall assume that $\beta-\alpha<e$.

iii. α and β even, $e+\varepsilon=1$. (19) yields $ad'+x'^2-\delta'y^2\equiv 0 \pmod{2^{\alpha+1}}$.

and $x=2^{\frac{\alpha}{2}}x'$; hence $2^{\beta-\alpha}ad'+x'^2-\delta'y^2\equiv 0 \pmod{2}$ which is solvable.

iv. α and β even, $e+\varepsilon=2$ (whence $\beta=\alpha$). When $\delta'\equiv 1 \pmod{4}$ we have $2^{\beta-\alpha}ad'+x'^2-\delta'y^2\equiv ad'+x'^2-y^2\equiv 0 \pmod{4}$ is solvable if and only if $ad'\not\equiv 2 \pmod{4}$. When $\delta'\equiv 3 \pmod{4}$, $\varepsilon=0$ and $2^{\beta-\alpha}ad'+x'^2-\delta'y^2\equiv ad'+x'^2+y^2\equiv 0 \pmod{4}$ is solvable if and only if $ad'\not\equiv 1 \pmod{4}$. Hence we have (1) of Theorem 15.

v. α and β even, $e + \varepsilon > 2$. (19) yields, as before, $2^{\beta-\alpha}ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon}}$. When $\alpha = \beta$, this congruence is solvable only if it has a solution modulo 8. But $ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{8}$ is easily seen to have solutions for all values of ad' and δ' modulo 8 except for those listed in case (2) of Theorem 15. But if the congruence is solvable modulo 8 it is solvable modulo $2^{e+\varepsilon}$. For, it is obvious that either x' or y is odd. If $ad' + x_0^2 - \delta'y_0^2 \equiv 0 \pmod{8}$ with x_0 odd, the congruence $x^2 \equiv \mu \pmod{8}$, $\mu = \delta'y_0^2 - ad'$, is solvable, whence there exists x_1 such that $x_1^2 \equiv \mu \pmod{2^{e+\varepsilon}}$, since $\mu \equiv 1 \pmod{8}$. Hence $ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon}}$ is solvable. If y_0 is odd, there is a similar argument.

Let now $\beta - \alpha > 0$ and $\delta' \equiv 1 \pmod{8}$. If $\beta - \alpha > 2$ or if $\beta - \alpha = 2$, $\varepsilon = 1$, $2^{\beta-\alpha}ad' + x'^2 - \delta'y^2 \equiv x'^2 - y^2 \equiv 0 \pmod{8}$ is solvable. But if $\beta - \alpha = 2$ and $\varepsilon = 0$, x' and y must both be even, $x' = 2\bar{x}$, $y = 2y'$, and our congruence becomes $ad' + \bar{x}^2 - \delta'y'^2 \equiv 0 \pmod{2^{e-2}}$. If $e = 3$ or 4 this congruence is solvable, but if $e > 4$ we have the first part of this case and the congruence is solvable since $\varepsilon = 0$.

Let $\delta' \not\equiv 1 \pmod{8}$. If $\delta' \equiv 3 \pmod{4}$ the congruence $2^{\beta-\alpha}ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon}}$ implies that x' and y must be even, for $x'^2 - 3y^2$ or $x'^2 - 7y^2$ can be $\equiv 0 \pmod{4}$ if and only if x' and y are even. If $\delta' \equiv 5 \pmod{8}$ and $\beta - \alpha > 2$ or if $\beta - \alpha = 2$, $\varepsilon = 1$, the same conclusion holds, but it fails to hold if $\beta - \alpha = 2$, $\varepsilon = 0$, for we may take $x' \equiv y \equiv 1 \pmod{8}$. In this last case, however, the congruence $2^{\beta-\alpha}ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon}}$ is solvable, since it is solvable modulo 8 with $x'y$ odd. In what follows, then we do not consider the case $\delta' \equiv 5 \pmod{8}$, $\varepsilon = 0$.

We write $x' = 2\bar{x}$, $y = 2y'$, and we have $2^{\beta-\alpha-2}ad' + \bar{x}^2 - \delta'y'^2 \equiv 0 \pmod{2^{e+\varepsilon-2}}$. If $\beta - \alpha - 2 \geq 2$, we can conclude, as before, that $\bar{x}$ and y' are even and repeat the argument. Continuing this process, we arrive ultimately at the congruence

$$2^{\beta-\alpha-2\gamma}ad' + \xi^2 - \delta'\eta^2 \equiv 0 \pmod{2^{e+\varepsilon-2\gamma}},$$

where the process has ended, that is, we have (since $\beta - \alpha$ is even and is $< e$)

- either
- 1) $e + \varepsilon - 2\gamma = 1$ (whence $\beta - \alpha - 2\gamma = 0$),
- or
- 2) $e + \varepsilon - 2\gamma = 2$, $\beta - \alpha - 2\gamma = 0$ ($e + \varepsilon = \beta - \alpha + 2$),
- or
- 3) $e + \varepsilon - 2\gamma \geq 3$, $\beta - \alpha - 2\gamma = 0$ ($e + \varepsilon \geq \beta - \alpha + 3$).

In (1) we have $\varepsilon = 0$ since $\beta - \alpha < e$, whence $e = 1 + \beta - \alpha$. But then $ad' + \xi^2 - \delta'\eta^2 \equiv 0 \pmod{2}$, which is certainly solvable.

In (2) we have $ad' + \xi^2 - \delta'\eta^2 \equiv 0 \pmod{4}$. The conditions for the solvability of this congruence are given in (3) and (4) of Theorem 15.

In (3) we have $ad' + \xi^2 - \delta'\eta^2 \equiv 0 \pmod{8}$. The conditions for the solvability of this congruence are given in (2) of Theorem 15.

vi. α even, β odd, $e + \varepsilon = 2$. We get $2^{\beta-\alpha}ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{4}$. $\varepsilon \neq 1$ since otherwise $\beta - \alpha < 1$, which is impossible. Hence $\varepsilon = 0$, $\beta - \alpha = 1$, and the congruence $2 + x'^2 - \delta'y^2 \equiv 0 \pmod{4}$ is solvable if and only if $\delta' \equiv 3 \pmod{4}$. This yields (5) of Theorem 15.

vii. α even, β odd, $e + \varepsilon > 2$. When $\beta - \alpha = 1$, $\varepsilon = 0$, the congruence becomes $2ad' + x'^2 - \delta'y^2 \equiv 0 \pmod{2^e}$; this congruence is solvable only if solvable modulo 8 whence $\delta' \equiv 3 \pmod{4}$ and ad' must satisfy the conditions in (6) of Theorem 15. Since one of x' and y must be odd in the solution of the congruence modulo 8, the original congruence is solvable.

When $\beta - \alpha = \varepsilon = 1$, then $\delta' \equiv 1 \pmod{4}$ and the congruence is solvable when $\delta' \equiv 5 \pmod{8}$ since it is solvable modulo 8 with y odd. When $\delta' \equiv 1 \pmod{8}$ it is easily seen that x' and y must be even if a solution is to exist, $x' = 2\bar{x}$, $y = 2y'$, whence $\frac{1}{2}ad' + \bar{x}^2 - \delta'y'^2 \equiv 0 \pmod{2^{e+1}}$. This is solvable if $e = 2$ or 3 and when $e > 3$ the congruence $\frac{1}{2}ad' + x^2 - y^2 \equiv 0 \pmod{8}$ is solvable so that the original congruence is also.

When $\beta - \alpha > 1$, $\beta - \alpha \equiv 3$ and modulo 8 the congruence implies $x'^2 - \delta'y^2 \equiv 0 \pmod{8}$. When $\delta' \equiv 1 \pmod{8}$ the original congruence is solvable since we may take $x'y$ odd, but when $\delta' \not\equiv 1 \pmod{8}$ x' and y must be even as is seen from the similar situation in case v. Applying the method there employed, we see that the congruence in question is solvable if and only if the congruence $2^{\beta-\alpha-2\gamma}ad' + x^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon-2\gamma}}$ is solvable, where either (since $\beta - \alpha$ is odd and is $< e$).

$$1) \quad e + \varepsilon - 2\gamma = 2, \quad \beta - \alpha - 2\gamma = 1 \quad (\text{whence } \varepsilon = 0, e = 1 + \beta - \alpha).$$

$$\text{or } 2) \quad e + \varepsilon - 2\gamma \equiv 3, \quad \beta - \alpha - 2\gamma = 1 \quad (\text{whence } e \equiv 2 + \beta - \alpha - \varepsilon).$$

In 1) the congruence is $2ad' + x^2 - \delta'y^2 \equiv 0 \pmod{4}$, which is easily seen to be solvable if and only if $\delta' \equiv 3 \pmod{4}$.

In 2) the congruence is $2ad' + x^2 - \delta'y^2 \equiv 0 \pmod{8}$, which is solvable only under the following conditions: $\delta' \equiv 3 \pmod{8}$, $ad' \equiv 1 \pmod{4}$; $\delta' \equiv 5 \pmod{8}$, $ad' \equiv 2 \pmod{4}$; $\delta' \equiv 7 \pmod{8}$, $ad' \equiv 3 \pmod{4}$. $\frac{\alpha+1}{2}$

viii. $\alpha\beta$ odd, $e + \varepsilon = 1$. Since in (19) $x^2 \equiv 0 \pmod{2^\alpha}$, $x = 2^{\frac{\alpha+1}{2}}x'$. Therefore, $2^{\beta-\alpha}ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{2}$; this congruence is always solvable since δ' is odd. $\frac{\alpha+1}{2}$

ix. $\alpha\beta$ odd, $e + \varepsilon = 2$. Again $x = 2^{\frac{\alpha+1}{2}}x'$ and we have $2^{\beta-\alpha}ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{4}$. This congruence is always solvable.

x. $\alpha\beta$ odd, $e + \varepsilon > 2$. Again we have $2^{\beta-\alpha}ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+\varepsilon}}$. This congruence is solvable only if it is solvable modulo 8, and a solution modulo 8 with y odd implies a solution modulo $2^{e+\varepsilon}$. If $\beta - \alpha = \varepsilon = 0$ we have the

congruence $ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{8}$ and y must be odd. For each odd value of δ' modulo 8 we find the possible values of ad' modulo 8; these possibilities are listed in (8) of Theorem 15. If $\varepsilon=1$, it follows that y is even, $y=2y'$ and we have $\frac{1}{2}ad' + x'^2 - 2\delta'y'^2 \equiv 0 \pmod{2^{e+\varepsilon-1}}$. When $e=2$, this congruence is always solvable with x' odd but when $e \geq 3$ only under the condition $ad' \equiv \pm 2 \pmod{16}$.

Let, now, $\beta - \alpha > 0$. Then y is even, $y=2y'$, and we have $2^{\beta-\alpha-1}ad' + x'^2 - 2\delta'y'^2 \equiv 0 \pmod{2^{e+\varepsilon-1}}$; then $x'=2\bar{x}$ and we have $2^{\beta-\alpha-2}ad' + 2\bar{x}^2 - \delta'y'^2 \equiv 0 \pmod{2^{e+\varepsilon-2}}$. Proceeding in this manner, we arrive at a congruence $2^{\beta-\alpha-2\gamma}ad' + 2\bar{\xi}^2 - \delta'\eta^2 \equiv 0 \pmod{2^{e+\varepsilon-2\gamma}}$ where $\beta - \alpha - 2\gamma = 0$ and either

$$1) \quad e + \varepsilon - 2\gamma = 1,$$

$$\text{or } 2) \quad e + \varepsilon - 2\gamma = 2,$$

$$\text{or } 3) \quad e + \varepsilon - 2\gamma \geq 3.$$

We assume first that $\varepsilon=0$. The congruences in the first two cases are $ad' + 2\bar{\xi}^2 - \delta'\eta^2 \equiv 0$ modulo 2 and 4, respectively, and these are solvable. For the last case, we get $ad' + 2\bar{\xi}^2 - \delta'\eta^2 \equiv 0 \pmod{8}$, which is solvable only under the conditions given in Theorem 15.

When $\varepsilon=1$, we can go one step further and get $\frac{1}{2}ad' + \bar{\xi}^2 - 2\delta'\eta'^2 \equiv 0 \pmod{2^{e-2\gamma}}$. When $e-2\gamma=e-(\beta-\alpha)=1$ or 2 this congruence is solvable, but when $e \geq 3 + \beta - \alpha$ we get, as above, that the condition to be satisfied is $ad' \equiv \pm 2 \pmod{16}$.

xi. α odd, β even, $e + \varepsilon = 2$. The congruence is $2^{\beta-\alpha}ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{4}$. Since $\beta - \alpha$ is odd and $< e$, $e=2$, $\varepsilon=0$, and $\beta - \alpha=1$. Hence the congruence in question becomes $2 + 2x'^2 - \delta'y^2 \equiv 0 \pmod{4}$, which has the solution $x' \equiv 1, y \equiv 0 \pmod{2}$.

xii. α odd, β even, $e + \varepsilon = 3$. The congruence now is $2^{\beta-\alpha}ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{8}$. Again $\beta - \alpha = 1$ and we have $2ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{8}$; since, then, $y=2y'$, we get $ad' + x'^2 - 2\delta'y'^2 \equiv 0 \pmod{4}$, which is solvable.

xiii. α odd, β even, $e + \varepsilon > 3$. We assume first that $\beta - \alpha = 1$, $\varepsilon=0$; we have, then, the congruence $2ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{2^e}$ or $ad' + x'^2 - 2\delta'y'^2 \equiv 0 \pmod{2^{e-1}}$. Since x' must be odd, we get $ad' + 1 - 2\delta'y'^2 \equiv 0 \pmod{8}$ whence $ad' \equiv 7$ or $2\delta' - 1 \pmod{8}$ according as y' is even or odd.

Let, now, $\beta - \alpha = \varepsilon = 1$. We have $2ad' + 2x'^2 - \delta'y^2 \equiv 0 \pmod{2^{e+1}}$ whence $\frac{1}{2}ad' + 2x''^2 - \delta'y'^2 \equiv 0 \pmod{2^{e-1}}$. This congruence is solvable for $e=3$ but for $e \geq 4$ the conditions of the theorem must be satisfied.

Let, now, $\beta - \alpha > 1$. Then $y = 2y'$, $x' = 2\bar{x}$ (as before) and we have $2^{\beta - \alpha - 2}ad' + 2\bar{x}^2 - \delta'y'^2 \equiv 0 \pmod{2^{\epsilon + \epsilon - 2}}$. Continuing this process we get ultimately a congruence $2^{\beta - \alpha - 2\gamma}ad' + 2\bar{\xi}^2 - \delta'\eta'^2 \equiv 0 \pmod{2^{\epsilon + \epsilon - 2\gamma}}$, where $\beta - \alpha - 2\gamma = 1$ and either

$$1) \quad c + \varepsilon \rightarrow 2\gamma = 2,$$

or 2) $e + \varepsilon - 2\gamma = 3$,

or 3) $e + \varepsilon - 2\gamma \geq 4$.

The congruences in cases (1) and (2) are solvable. The congruence in case (3) is $2ad' + 2\xi^2 - \delta'\eta^2 \equiv 0 \pmod{2^{e+\varepsilon-2r}}$ and when $\varepsilon=0$ we have $ad' + \xi^2 - 2\delta'\eta^2 \equiv 0 \pmod{8}$, which is solvable only when $ad' \equiv \pm 1 \pmod{8}$ for $\delta' \equiv 1 \pmod{4}$ and $ad' \equiv 5, 7 \pmod{8}$ when $\delta' \equiv 3 \pmod{4}$.

When $\varepsilon=1$, we get $\frac{1}{2}ad'+2\xi^2-\delta'\eta^2\equiv 0 \pmod{2^{e-1-2r}}$ and we find that modulo 8 this congruence is satisfied under the following conditions: $ad'\equiv \pm 2 \pmod{16}$ for $\delta'\equiv 1 \pmod{8}$, and $ad'\equiv \pm 6 \pmod{16}$ for $\delta'\equiv 5 \pmod{8}$.

11. *Proper representations of $k\varphi$ by $\Sigma(kd)$.* We are now ready to complete the discussion of the proper representation of $k\varphi$ by $\Sigma(kd)$, where φ is primitive, of determinant δ , and a section of the set $\Sigma(d)$.

Write $k=2^{e_1}p_1^{e_2}\dots p_n^{e_u}$, where the p_i are distinct odd primes and $e\equiv 0$; and write $\delta=2^{\alpha_1}\alpha_1^{p_2}\dots p_v^{\alpha_v}P$, where P is prime to k , and $v\equiv u$. By the preceding sections, the congruences

$$d + ar^2 + bs^2 - 2rst \equiv 0 \pmod{2^{e+\alpha}}$$

$$d + ar_1^2 + bs_1^2 - 2r_1s_1t \equiv 0 \pmod{p_1^{e_1+\alpha_1}}$$

$$(2I) \quad d + ar_v^2 + bs_v^2 - 2\alpha_v d \equiv 0 \pmod{p_v^{e_v + \alpha_v}}$$

$$d + ar_{v+1}^2 + bs_{v+1}^2 - 2r_{v+1}s_{v+1}t \equiv 0 \pmod{p_{v+1}^{e_{v+1}}}$$

• • • • •

$$d + ar_u^2 + bs_u^2 - 2r_us_ut \equiv 0 \pmod{p_u^e}$$

$$d + ar'^2 + bs'^2 - 2r's't \equiv 0 \pmod{P}$$

will have solutions if and only if the Theorems 11--15 are satisfied for the various primes dividing δ, d and k . But if these theorems do hold, then, since the $u+2$ congruences (21) have relatively prime moduli, there exist integers ρ, σ , such that

$$d + ap^2 + b\sigma^2 - 2p\sigma t \equiv 0 \pmod{k\delta}$$

whence, by Lemma 5, $k\varphi$ is a section of $\Sigma(kd)$.

Conversely, if $k\varphi$ is represented properly by $\Sigma(kd)$, the congruences (21) will be simultaneously solvable, so that we have the

THEOREM 16. *Let $k\varphi$ be a classic binary form, where φ is assumed to be primitive. Let p^e be the highest power of a prime p dividing k . Then $k\varphi$ is a section of a set $\Sigma(d)$ if and only if $d \equiv 0 \pmod{k}$, φ is a section of $\Sigma(d/k)$, and $p^e\varphi$ is a section of $\Sigma(p^e d/k)$, for every such prime-power factor p^e of k .*

THE UNIVERSITY OF CHICAGO.

VITA

Daniel Maccabaeu Dribin was born on December 10, 1913. He received his elementary and high-school education in the Chicago public schools and in April, 1930, entered the University of Chicago, from which institution he was graduated in 1933 with the S.B. degree. In August, 1934, he received the degree of Master of Science. He spent the years 1935-36 as a University Fellow.

As a graduate student he pursued courses taught by Professors Albert, Barnard, Bartky, Bliss, Dickson, Graves, Hestenes, Lane, Lunn, MacMillan, and Reid. To Professor Albert especially he wishes to express his thanks for the valuable advice received in the preparation of this dissertation.

